<div align="center">**PROTECTION FOR**

CONTROLLED UNCLASSIFIED INFORMATION</div>

General: There are types of information that are not classified, but which require protective measures which restrict its distribution for a variety of reasons. This information is known as "controlled unclassified information (CUI)." The types of information considered CUI for the program are information marked "For Official Use Only" by the U.S. Government and Technical Data. When handling CUI material, all personnel are to comply with these requirements and follow their company policy and/or applicable Proprietary Information Agreements (PIAs) concerning the protection of proprietary information in situations not clearly stated herein.

Technical Data Description: Any recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul program material. The data may be graphic or pictorial delineations in media, such as computer software, drawings or photographs, text in specifications, or related performance or design documents, or computer printouts. Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and related information, and computer software documentation.

FOR OFFICIAL USE ONLY INFORMATION (FOUO) Description: "For Official Use Only (FOUO)" is a Government designation that is applied to **unclassified** information that may be exempt from mandatory release to the public under the Freedom of Information Act. FOUO information includes information identified as such in the Security Classification Guide or information from a government document marked FOUO.

CUI Markings

Marking of FOUO documents will be in accordance with Army Regulation 25-55. (http://www.apd.army.mil/pdffiles/r25_55.pdf). Information extracted from an FOUO document will carry the FOUO marking until formally reviewed by the government.

Marking of unclassified Technical Data will, at a minimum include the statements listed below. This does not preclude additional mandated markings as may be required by the contract such as Competition Sensitive Information.

Government Distribution Statement: Unless otherwise directed by the government Security Manager, the below Distribution Statement F is required on all Technical Data delivered to the government.

> DISTRIBUTION STATEMENT F: Further distribution only as directed by PEO Integration Security Office, ATTN: SFAE-INT-CSC/MS 515, 6501 East Eleven Mile Road, Warren, MI 48397-5000, 8 January 2010.

Export Warning Statement: Technical Data contained in documents not approved for export shall display the appropriate export control caveat on the front cover or title page, as follows:

> **"WARNING** - This document contains technical data whose export may be restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq) or the Export Administration Act of 1979, as amended (Title 50, U.S.C., App. 2401 et seq). Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25."

Protection of CUI Information

Access: Program CUI is restricted to personnel with a valid need to know the information, unless public release authorization has been obtained. Information, in any media format may only be disseminated on a need to know basis. The need to know restricts the use or dissemination of CUI data to those individuals

or organizations with direct affiliation with the given program or project. Further dissemination of such information will be at the discretion of the government Security Manager. Personnel no longer requiring access to CUI must delete or surrender any in their possession and terminate future access to it.

Storing/Handling: During working hours, reasonable steps should be taken to minimize risk of access to CUI by unauthorized personnel. After working hours, CUI information shall be stored in locked desks, file cabinets, bookcases, locked rooms, or similar means. CUI may not be displayed in public places, such as airports, airplanes, restaurants, etc. Computers used for processing CUI do not need to be accredited for classified use. Do not process DoD information on public computers (e.g. those available for use by the general public in kiosks, hotel business centers or the like) or computers that do not have access control. Personally owned computers are not authorized for processing CUI. Program CUI stored electronically on all devices such as company issued laptops, Personal Digital Assistants (PDA), and removable media, are to be physically protected or protected using cryptographic products that are either NIST approved or comply with FIPS 140-2. Protect CUI by at least one physical or electronic barrier when not under direct individual control.

Dissemination: CUI printed documents and material may be transmitted through mail channels or handcarried without formal courier orders. Use of secure communications whenever possible; however, land-line communications for telephone conversations are more secure than cellular and should be utilized whenever available for program CUI discussions. Voice and fax transmissions will be transmitted only when the sender has a reasonable assurance that only authorized recipients will have access to the transmission. For digital transmission, the following guidelines apply:

▪ Collaborative suites may be used by personnel not located on a government backbone (i.e., NIPRNET) without Government Security Office approval provided all of the following requirements apply:

➢ Use only NIST approved cryptographic vendors and algorithms. The latest validation lists may be obtained at: http://csrc.nist.gov/cryptval/ and,

➢ An internally hosted service (does not use third-party collaborative suite service provider) and, (excluding currently approved collaborative tools pending final Government determination).

➢ Notify the Government Security Office, in writing, of the collaborative suite and version.

▪ Personnel with access to NIPRNET require local Designated Approving Authority (DAA) approval prior to participation in any collaborative suite that requires **installation of mobile code** on the local NIPRNET connected system.

▪ All computers containing program CUI must be protected by either physical isolation from all personnel without a valid need for the information or protected using cryptographic products that are either NIST approved or comply with FIPS 140-2 Discretionary access control measures must be used to preclude access to CUI data by authorized users but who are not authorized access to CUI information. After working hours, when not in physical possession of the owner, all electronic assets containing program CUI must be afforded a reasonable degree of physical protection to prevent theft of program information i.e. locking up laptops or cable locking them to a stationary base.

▪ All transmission/dissemination of CUI identified with a Distribution Statement or marked FOUO (i.e. email and file transfers) must use applications utilizing NIST approved cryptographic vendors and algorithms. The latest validation lists may be obtained at: http://csrc.nist.gov/cryptval/. This encryption requirement includes passcodes to teleconferences or VIS/iMeeting where there is a reasonable expectation that CUI may be discussed. When encryption is not available, CUI will not be transmitted electronically. Encrypt all wireless external data connections.

▪ Do not post CUI to web pages that are publically available or have access limited only by domain/IP restrictions. As permitted by other contract provisions, CUI may be posted to web pages that control access by user ID/ Password, user certificates, or other technical means, and which provide protection via use of secure sockets, or other equivalent technologies. Access control may be provided by the intra-net (vice the website itself or the website it hosts).

- External transmission/dissemination of CUI (i.e. email and file transfers) to or from a DoD computer shall be encrypted by use of a DoD approved Public Key Infrastructure Certification. These are available from: http://iase.disa.mil/pki/eca/iecavendors.html.

- As new technologies become available in the electronics arena care should be given to providing a reasonable degree of protection to program information from known vulnerabilities.

- Internet shall be equated with "Public Access". Therefore, CUI must be reviewed and officially approved for public release before placing on the Internet. This is not applicable when the internet is used for e-mail transmissions and encryption is used as noted above.

Disposal: CUI documents shall be destroyed by cross-cut shredding or equivalent tearing into pieces so as not to be easily reconstructed. CUI on removable media and computing devices must be cleared (e.g., overwriting memory locations, degaussed) before being disposed of or transferred to another program. Removable media and computing devices may also be disposed of by providing them to a company's internal organization responsible for destruction. Sanitize CUI with a three-time overwrite before sale, transfer, or reassignment to those not authorized and requiring access to data stored thereon.

Report of Loss of CUI: Contractors will notify government Security Manager of any loss of CUI.

Intrusions or incidents involving the potential compromise, exfiltration, or other loss of CUI, on a contractor information system shall be reported.

Electronic initial reports shall be made as expeditiously as possible in all cases within 72 hours of discovery. Initial report content shall include the following information as available.

- Applicable dates, including dates of compromise and dates of discovery

- Threat methodology, including all known resources used (e.g. IP addresses, domain names, software tools)

- Account of what actions the threat(s) may have taken on victim system/network

- What information may have been compromised exfiltrated or lost and its potential impact on government programs

Report of Cyber Intrusions: As soon as Contractors learn of them, report cyber intrusions and other compromises of Defense Program Information (DPI) to their supporting counterintelligence office, which will inform the DoD-DIB Common Information Sharing Environment (DCISE). The Contractor will also notify the government Security Manager of any incidents.